

CLAIMS

What is claimed is:

- 1 1. A method of duplicating electronic data from a source storage device to a
2 target storage device, comprising:
3 detecting a presence of a host protected area of a source storage device; and
4 copying data included in the host protected area of the source storage device
5 to a host protected area of a target storage device.
- 1 2. The method as described in claim 1, further comprising determining size of
2 the host protected area of the source storage device.
- 1 3. The method as described in claim 2, further comprising creating a host
2 protected area on the target storage device of a size corresponding to the
3 determined size of the host protected area of the source storage device.
- 1 4. The method as described in claim 3, wherein the size of the host protected
2 area of the target storage device is suitable for at least one of including the
3 host protected area of the source storage device, including the host protected
4 area of the source storage device and at least a portion of a previously stored
5 host protected area data of the target storage device.
- 1 5. The method as described in claim 1, further comprising creating a host
2 protected area on the target storage device suitable for storing host protected
3 area data from the source storage device.
- 1 6. The method as described in claim 1, wherein a previously stored host
2 protected area of the target storage device is overwritten by the host protected
3 area of the source storage device.

1 7. The method as described in claim 1, further comprising copying user
2 accessible data from the source storage device to the target storage device, the
3 user accessible data stored on a user accessible area of the target storage
4 device.

1 8. The method as described in claim 1, further comprising detecting a presence
2 of a host protected area on the target storage device, and if a host protected
3 area is present, resetting the host protected area of the target storage device.

1 9. The method as described in claim 8, wherein the host protected area is
2 detected utilizing a EC and READ NATIVE MAX CYL command and the
3 host protected area is reset utilizing a SET MAX CYL command.

1 10. The method as described in claim 1, wherein the presence of a host protected
2 area is detected utilizing a READ NATIVE MAX CYL command.

1 11. A method of duplicating electronic data from a source storage device to a
2 target storage device, comprising:

3 detecting presence of a host protected area of a source storage device;
4 determining size of the host protected area of the source storage device;
5 creating a host protected area on a target storage device of a size
6 corresponding to the determined size of the host protected area of the
7 source storage device; and
8 copying data included in the host protected area of the source storage device
9 to the created host protected area of the target storage device.

1 12. The method as described in claim 11, wherein the size of the host protected
2 area of the target storage device is suitable for at least one of including the
3 host protected area of the source storage device, including the host protected
4 area of the source storage device and at least a portion of a previously stored
5 host protected area data of the target storage device.

1 13. The method as described in claim 11, wherein the creates host protected area
2 on the target storage device is suitable for storing host protected area data
3 from the source storage device.

1 14. The method as described in claim 11, wherein creating a host protected area
2 on the target storage device includes overwriting a previously stored host
3 protected area of the target storage device by the host protected area of the
4 source storage device.

1 15. The method as described in claim 11, further comprising copying user
2 accessible data from the source storage device to the target storage device, the
3 user accessible data stored on a user accessible area of the target storage
4 device.

1 16. The method as described in claim 11, further comprising detecting a presence
2 of a host protected area on the target storage device, and if a host protected
3 area is present, resetting the host protected area of the target storage device
4 to create the host protected area of the target storage device suitable for
5 storing host protected area data from the source storage device.

1 17. The method as described in claim 16, wherein the host protected area is
2 detected utilizing a READ NATIVE MAX CYL command and the host
3 protected area is reset utilizing a SET MAX CYL command.

1 18. The method as described in claim 11, wherein the presence of a host protected
2 area is detected utilizing a READ NATIVE MAX CYL command.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50

1 19. A method of duplicating electronic data from a source storage device to a
2 target storage device, comprising:

3 detecting presence of a host protected area of a source storage device;
4 creating a host protected area on a target storage device suitable for storing
5 host protected area data from the source storage device; and
6 copying data included in the host protected area of the source storage device
7 to the created host protected area of the target storage device.

1 20. The method as described in claim 19, further comprising determining size of
2 the host protected area of the source storage device.

1 21. The method as described in claim 20, wherein a host protected area on the
2 target storage device is created of a size corresponding to the determined size
3 of the host protected area of the source storage device.

1 22. The method as described in claim 21, wherein the size of the host protected
2 area of the target storage device is suitable for at least one of including the
3 host protected area of the source storage device, including the host protected
4 area of the source storage device and at least a portion of a previously stored
5 host protected area data of the target storage device.

1 23. The method as described in claim 19, wherein a previously stored host
2 protected area of the target storage device is overwritten by the host protected
3 area of the source storage device.

1 24. The method as described in claim 19, further comprising copying user
2 accessible data from the source storage device to the target storage device, the
3 user accessible data stored on a user accessible area of the target storage
4 device.

1 25. The method as described in claim 19, further comprising detecting a presence
 2 of a host protected area on the target storage device, and if a host protected
 3 area is present, resetting the host protected area of the target storage device to
 4 create the host protected area of the target storage device suitable for storing
 5 host protected area data from the source storage device.

1 26. The method as described in claim 25, wherein the host protected area is
 2 detected utilizing a READ NATIVE MAX CYL command and the host
 3 protected area is reset utilizing a SET MAX CYL command.

1 27. The method as described in claim 19, wherein the presence of a host protected
 2 area is detected utilizing a READ NATIVE MAX CYL command.

3 detecting presence of a host protected area of a source storage device;
4 detecting a presence of a host protected area on a target storage device, and if
5 a host protected area is present, resetting the host protected area of the
6 target storage device; and
7 copying data included in the host protected area of the source storage device
8 to the host protected area of the target storage device.

1 29. The method as described in claim 28, further comprising determining size of
2 the host protected area of the source storage device.

1 30. The method as described in claim 29, wherein the host protected area on the
2 target storage device is reset to a size corresponding to the determined size of
3 the host protected area of the source storage device.

1 31. The method as described in claim 30, wherein the size of the host protected
2 area of the target storage device is suitable for at least one of including the
3 host protected area of the source storage device, including the host protected
4 area of the source storage device and at least a portion of a previously stored
5 host protected area data of the target storage device.

32. The method as described in claim 29, further comprising creating a host
protected area on the target storage device suitable for storing host protected
area data from the source storage device.

1 33. The method as described in claim 29, wherein a previously stored host
2 protected area of the target storage device is overwritten by the host protected
3 area of the source storage device.

1 34. The method as described in claim 29, further comprising copying user
2 accessible data from the source storage device to the target storage device, the
3 user accessible data stored on a user accessible area of the target storage
4 device.

1 35. The method as described in claim 29, wherein the host protected area is
2 detected utilizing a READ NATIVE MAX CYL command and the host
3 protected area is reset utilizing a SET MAX CYL command.

1 36. The method as described in claim 29, wherein the presence of a host protected
2 area is detected utilizing a READ NATIVE MAX CYL command.

- 1 37. A storage device duplication system, comprising:
2 a source storage device suitable for storage of electronic data, the source
3 storage device including a host protected area ;
4 a target storage device suitable for storing electronic data; and
5 a duplicating machine communicatively coupled to the source storage device
6 and the target storage device, wherein the duplicating machine detects
7 the presence of the host protected area of the source storage device and
8 copies data included in the host protected area of the source storage
9 device to a host protected area of the target storage device.
- 1 38. The system as described in claim 37, wherein the duplicating machine
2 determines a size of the host protected area of the source storage device and
3 creates a host protected area on the target storage device of a size
4 corresponding to the determined size of the host protected area of the source
5 storage device.
- 1 39. The system as described in claim 38, wherein the size of the host protected
2 area of the target storage device is suitable for at least one of including the
3 host protected area of the source storage device, including the host protected
4 area of the source storage device and at least a portion of a previously stored
5 host protected area data of the target storage device.
- 1 40. The system as described in claim 38, wherein the duplicating machine creates
2 a host protected area on the target storage device suitable for storing host
3 protected area data from the source storage device.
- 1 41. The system as described in claim 38, wherein a previously stored host
2 protected area of the target storage device is overwritten by the host protected
3 area of the source storage device.

1 42. The system as described in claim 38, wherein the duplicating machine copies
 2 user accessible data from the source storage device to the target storage
 3 device, the user accessible data stored on a user accessible area of the target
 4 storage device.

1 43. The system as described in claim 38, wherein the duplicating machine detects
 2 a presence of a host protected area on the target storage device, and if a host
 3 protected area is present, resets the host protected area of the target storage
 4 device.

1 44. The system as described in claim 43, wherein the host protected area is
 2 detected utilizing a READ NATIVE MAX CYL command and the host
 3 protected area is reset utilizing a SET MAX CYL command.

1 45. The system as described in claim 38, wherein the presence of a host protected
 2 area is detected utilizing a READ NATIVE MAX CYL command.

- 1 46. An electronic data duplication system, comprising:
2 means for storing a source of electronic data, the source storage means
3 including a means for protecting host data;
4 means for storing target storage electronic data; and
5 means for duplicating electronic data communicatively coupled to the source
6 storage means and the target storage means, wherein the duplicating
7 means detects the presence of the host data protection means of the
8 source storage means and copies data included in the host data
9 protection means of the source storage means to a host data protection
10 means of the target storage means.
- 1 47. The system as described in claim 46, wherein the duplicating means
2 determines a size of the host data protection means of the source storage
3 means and creates a host data protection means on the target storage means of
4 a size corresponding to the determined size of the host data protection means
5 of the source storage means.
- 1 48. The system as described in claim 47, wherein the size of the host data
2 protection means of the target storage means is suitable for at least one of
3 including the host data protection means of the source storage device,
4 including the host data protection means of the source storage device and at
5 least a portion of a previously stored host data protection means data of the
6 target storage device.
- 1 49. The system as described in claim 46, wherein the duplicating means creates a
2 host data protection means on the target storage means suitable for storing
3 host data protection means data from the source storage means.
- 1 50. The system as described in claim 46, wherein a previously stored host data

2 protection means of the target storage means is overwritten by the host data
3 protection means of the source storage means.

1 51. The system as described in claim 46, wherein the duplicating means copies
2 user accessible data from the source storage means to the target storage
3 means, the user accessible data stored on a user accessible area of the target
4 storage means.

1 52. The system as described in claim 46, wherein the duplicating means detects a
2 presence of a host data protection means on the target storage means, and if a
3 host data protection means is present, resets the host data protection means of
4 the target storage means.

1 53. The system as described in claim 52, wherein the host data protection means
2 is detected utilizing a READ NATIVE MAX CYL command and the host data
3 protection means is reset utilizing a SET MAX CYL command.

1 54. The system as described in claim 46, wherein the presence of a host data
2 protection means is detected utilizing a READ NATIVE MAX CYL
3 command.